

CLAIMS

What is claimed is:

1. A password strength checking method comprising:
inputting a password to be checked;
generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool;
determining whether or not the inputted password and the generated password candidate match each other;
directing generation of the next password candidate when the match is not determined;
determining strength of the inputted password based on the number of the generated password candidates when the match is determined; and
outputting information of the determined password strength.
2. The password strength checking method according to claim 1, wherein the inputting step presents the password input state to a user in a form that the inputted content is not readable, requests re-input of the password from the user, and inputs the password to be checked only when the inputted two passwords match each other.
3. The password strength checking method according to claim 1, wherein the inputting step also inputs user attribute information and controls strength checking not to be executed for the inputted password when the inputted user attribute information and the inputted password match each other.
4. The password strength checking method according to claim 1, wherein the determining step estimates a time required for the password guessing tool to attack

the password to be checked based on the number of the generated password candidates to determine the time as a password strength.

5. The password strength checking method according to claim 1, wherein the determining step calculates numerical information based on a ratio value of the possible maximum number of the password candidates to be generated and the number of the generated password candidates to determine the numerical information as a password strength.

6. The password strength checking method according to claim 1, wherein outputting step further outputs information of a rank among passwords, which have been checked and for which password strength has been determined, which is identified based on the determined password strength.

7. A password strength checking apparatus comprising:

means for inputting a password to be checked;

means for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool;

means for determining whether or not the inputted password and the generated password candidate match each other;

means for directing generation of the next password candidate when the match is not determined;

means for determining strength of the inputted password based on the number of the generated password candidates when the match is determined; and

means for outputting information of the determined password strength.

8. A program for checking password strength executed in a computer, wherein the program causes a computer to execute:

inputting a password to be checked;

generating a plaintext password candidate according to the same generation procedure used by a password guessing tool;

determining whether or not the inputted password and the generated password candidate match each other;

directing generation of the next password candidate when the match is not determined;

determining strength of the inputted password based on the number of the generated password candidates when the match is determined; and

outputting information of the determined password strength.

9. A recording medium recording a password strength checking program, wherein the program causes a computer to execute:

inputting a password to be checked;

generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool;

determining whether or not the inputted password and the generated password candidate match each other;

directing generation of the next password candidate when the match is not determined;

determining strength of the inputted password based on the number of the generated password candidates when the match is determined; and

outputting information of the determined password strength.

10. A password creation assisting method comprising:

inputting a password to be targeted by creation assistance and characters' places information for identifying a character string to be checked that is included in the password;

using a password candidate generating tool for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool to obtain the number of password candidates which have been generated by the time a password candidate having the character string at the characters' places is first generated;

calculating strength of the character string based on the obtained number of generated password candidates; and

outputting the calculated character string strength information.

11. A password creation assisting method comprising:

inputting a password to be targeted by creation assistance;

extracting all or a part of characters composing the inputted password together with places of the characters;

identifying, for each of the extracted characters, a character rank at the extracted character position, with the extracted characters and the characters' places as a key, by referring to a table group recording character rank information for each character position, the table group being provided for a password guessing tool to use when guessing a password by checking all possible passwords;

calculating character strength for each of the extracted characters based on the identified character rank; and

outputting information of the calculated character strength.

12. A password creation assisting method comprising:

- inputting a password to be targeted by creation assistance;
- extracting character strings increasing in length by an increment of one character, with the first character of the inputted password as a top character;
- using a password candidate generating tool for generating a plaintext password candidate according to the same generation procedure used by a password guessing tool to obtain, for each of the extracted character strings, the number of password candidates which have been generated by the time a password candidate having the character string at the same characters' places is first generated;
- calculating a character strength transition value of the inputted password based on the obtained number of the generated password candidates; and
- outputting the calculated character strength transition value.

13. A program for assisting password creation executed in a computer, wherein the program causes a computer to execute:

- inputting a password to be targeted by creation assistance and characters' places information for identifying a character string to be checked that is included in the password;
- using a password candidate generating tool for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool to obtain the number of password candidates which have been generated by the time a password candidate having the character string at the characters' places is first generated;

- calculating strength of the character string based on the obtained number of generated password candidates; and

- outputting the calculated character string strength information.

14. A program for assisting password creation executed in a computer, wherein the program causes a computer to execute:

inputting a password to be targeted by creation assistance;

extracting all or a part of characters composing the inputted password together with places of the characters;

identifying, for each of the extracted characters, a character rank at the extracted character position, with the extracted characters and the characters' places as a key, by referring to a table group recording character rank information for each character position, the table group being provided for a password guessing tool to use when guessing a password by checking all possible passwords;

calculating character strength for each of the extracted characters based on the identified character rank; and

outputting the calculated character strength information.

15. A program for assisting password creation executed in a computer, wherein the computer causes a computer to execute:

inputting a password to be targeted by creation assistance;

extracting character strings increasing in length by an increment of one character, with the first character of the inputted password as a top character;

using a password candidate generating tool for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool to obtain, for each of the extracted character strings, the number of password candidates which have been generated by the time a password candidate having the character string at the same characters' places is first generated;

calculating a character strength transition value of the inputted password based on the obtained number of the generated password candidates; and
outputting the calculated character strength transition value.

16. A password creating method comprising:

inputting information of a generation rank for a password to be created;
using a password candidate generating routine for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool to obtain a password candidate generated for the generation rank by the password candidate generating routine; and
outputting the obtained password candidate as a password to be created.

17. A password creating method comprising:

inputting information indicating strength of a password to be created;
converting the information indicating strength into information of a generation rank of a password candidate to be generated by a password candidate generating routine for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool;
using the password candidate generating routine to obtain a password candidate generated for the generation rank by the password candidate generating routine; and
outputting the obtained password candidate as a password to be created.

18. The password creating method according to claim 16 or 17, wherein the obtaining step creates one or more generation ranks by changing the value of the generation rank randomly and in vicinity thereof to obtain password candidates

generated at the created generation ranks in addition to or instead of the generation rank.

19. The password creating method according to claim 16 or 17, wherein the outputting step determines whether or not the obtained password candidate matches any password outputted in the past and, if not, outputs the obtained password candidate as a password to be created.

20. The password creating method according to claim 16 or 17, wherein the outputting step determines whether or not the obtained password candidate matches any word registered with a dictionary and, if not, outputs the obtained password candidate as a password to be created.

21. A program for creating password executed in a computer, wherein the program causes a computer to execute:

- inputting information of a generation rank for a password to be created;
- using a password candidate generating routine for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool to obtain a password candidate generated for the generation rank by the password candidate generating routine; and
- outputting the obtained password candidate as a password to be created.

22. A program for creating password executed in a computer wherein the program causes a computer to execute:

- inputting information indicating strength of a password to be created;

converting the information indicating strength into information of a generation rank of a password candidate to be generated by a password candidate generating routine for generating a plaintext password candidate according to the same generation procedure as that used by a password guessing tool;

using the password candidate generating routine to obtain a password candidate generated for the generation rank by the password candidate generating routine; and

outputting the obtained password candidate as a password to be created.

23. The password creating program according to claim 21 or 22, wherein the obtaining process creates one or more generation ranks by changing the value of the generation rank randomly and in vicinity thereof to obtain password candidates generated at the created generation ranks in addition to or instead of the generation rank.